Application No. 10826745 (Docket: CNTR.2228)
37 CFR 1.111 Amendment dated 01/26/2008
Reply to Office Action of 10/12/2007

AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and

substitute the following section therefor:

SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and
other problems and disadvantages of the prior art. The present invention provides a
superior technique for performing cryptographic operations within a microprocessor. In
one embodiment, an apparatus in a microprocessor is provided for accomplishing
cryptographic operations. The apparatus includes a cryptographic instruction, OFB mode
logic, and execution logic. The cryptographic instruction is received by a ~~computing~~
~~device~~microprocessor as part of an instruction flow executing on the ~~computing~~
~~device~~microprocessor. The cryptographic instruction prescribes one of the cryptographic
operations. The one of the cryptographic operations includes a plurality of OFB block
cryptographic operations performed on a corresponding plurality of input text blocks.
The OFB mode logic is operatively coupled to the cryptographic instruction. The OFB
mode logic directs the ~~computing device~~microprocessor to update pointer registers and an
initialization vector location for each of the plurality of OFB block cryptographic
operations. The execution logic is operatively coupled to the OFB mode logic. The
execution logic executes the one of the cryptographic operations.

[0022] One aspect of the present invention contemplates a apparatus for performing
cryptographic operations. The apparatus includes a cryptography unit within a
~~device~~microprocessor, and OFB mode logic. The cryptography unit executes one of the
cryptographic operations responsive to receipt of a cryptographic instruction within an
instruction flow that prescribes the one of the cryptographic operations. The one of the
cryptographic operations includes a plurality of CFB block cryptographic operations
performed on a corresponding plurality of input text blocks. The OFB mode logic is
operatively coupled to the cryptography unit. The OFB mode logic directs the
~~device~~microprocessor to update pointer registers and an initialization vector location for
each of the plurality of OFB block cryptographic operations.

Application No. 10826745 (Docket: CNTR.2228)
37 CFR 1.111 Amendment dated 01/26/2008
Reply to Office Action of 10/12/2007

[0023] Another aspect of the present invention comprehends a method for performing cryptographic operations in a devicemicroprocessor. The method includes executing one of the cryptographic operations responsive to receiving a cryptographic instruction, wherein the cryptographic instruction prescribes the one of the cryptographic operations. The executing includes performing a plurality of OFB mode block operations on a corresponding plurality of input text blocks. The method also includes writing an initialization vector equivalent to an initialization vector location for employment by a following one of the plurality of OFB mode block operations on a following one of the plurality of input text blocks.